R9.5 Release Notes

Beta 2

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

R95 Release Notes - Beta 2

PowerShell

Added a PowerShell command line console to Live Connect. (EES-1071)

- The Commands menu in Live Connect now displays a drop-down menu with two options: Command Prompt and PowerShell.
- Selecting the PowerShell option displays a PowerShell command line interface you can use to run any PowerShell command and PS1 script on the remote machine.
- Supports using up and down keys to move around the PowerShell command line.
- Results, including errors, are returned to the PowerShell command line.

Folder Transfer

Multi-level folders can now be uploaded and downloaded between the local machine and remote agent machines using the Live Connect > File Manager interface. Previously only individual files could be copied. This feature is supported on both Windows and Mac, for both local and remote machines. (EES-1355)

Cloud Backup Profiles

Added a new Profiles page to the Cloud Backup module. Profiles are applied to agent machines and configure backup options deployed by the Acronis website. (EXT-2685)

In addition, a new Cloud Backup category was added to Policy Management. The new category provides two options. (EXT-2841)

- Backup profiles
- Alert profiles

Antivirus

The following reboot options were added to Antivirus profiles. (EXT-2748)

- When the user is logged in
  - ➢ Reboot immediately after update
  - ➢ Warn user and wait for x min and then reboot
  - ➢ Ask user about reboot and offer to delay (reask every x minute); do not reboot until get response
  - ➢ Ask permission, if no response in x min reboot
  - ➢ Skip Reboot
  - ➢ Do not reboot after update, send email - You can configure the email format using the Settings page.
- Wait time - Minutes to wait after warning the user of reboot.
- When a user is not logged in
  - ➢ Reboot immediately after update
  - ➢ Warn user and wait for x min and then reboot
  - ➢ Skip Reboot
  - ➢ Do not reboot after update, send email - You can configure the email format using the Settings page.

Software Management , released July 1, 2017

Software Management is a new vulnerability and patch management module for Windows and Apple machines. Software Management also manages deployment of popular 3rd-party software packages for both Windows and Apple operating systems. Patches for 3rd-party software is included, if made available by 3rd-party software package developers.

Scanning and deployment can be on demand or automated across thousands of machines. Settings are assigned to machines using profiles for scanning, deployment, alerts, 3rd-party software and patch overrides. Once profiles are assigned, policy enforcement is validated using compliance checking metrics for scanning and deployment.

- Scan and analysis profiles support two different *strategies* for managing software updates.
  - ➢ Configure Operating System Update - Configures how updates for Windows and Apple machines are performed on assigned machines. Individual Windows and Apple patches are not reviewed and selected using this option. *3rd-party patches cannot be deployed using this strategy.*
  - ➢ Kaseya Update - Specifies whether to approve, reject or review patches based on a pre-assigned *impact classification*. This patch strategy applies to Windows, Apple and 3rd-party software patches.
- Deployment profiles specify how deployments occur, on a recurring schedule. This includes:
  - ➢ Reboot preferences.
  - ➢ The optional running of agent procedures both before or after deployment.
  - ➢ Optional blackout windows, to prevent scheduling deployments during business hours.
- Includes patch approvals, which lets you approve or reject specific patches.
- Supports scanning and deploying patches immediately.
- Provides a *force update* feature, which initiates a scan, then deploys all installs and approved patches immediately, rebooting as often as necessary.
- 3rd-party software profiles enable you to maintain lists of popular software titles and versions that can be installed on agent machines.
  - ➢ A Software Management license is only incremented when 3rd-party software management is enabled for an agent machine.
  - ➢ 3rd-party software can only be installed by deployment profile.
  - ➢ Requires a scan and analysis profile be assigned to the agent machine that uses the Kaseya Update strategy.
- Patch override profiles—by KB article, patch number, and filter criteria—can be specified. When assigned to a machine, these profiles override the default classifications assigned to patches: approved, rejected, or review.
- Alerts are provided for patch and configuration issues.
- A daily compliance check is run for delayed scans, delayed deployments and percentage of patches deployed.
- Software Management activities are tracked using reports, application logs and diagnostic logs.

Additional Features

Agent	SDP-2817	The following new agent properties were added. • Purchase Date • Warranty Expiry Date
Kaseya Remote Control	EES-273	Session recordings were added to Kaseya Remote Control. A recording can be optional or required by policy. • When required by policy, the KRC recording button is enabled during the entire session and cannot be disabled. • When KRC recording is optional, the admin is able to record a session by starting and stopping the recording button.
Kaseya Remote Control	EES-1117	With this enhancement, starting and stopping the Recording... button multiple times during a KRC session creates individual recordings for each segment of the session you record.
Licensing	APPF-418	The license information in the notification bar and on the System > License Manager License tab now shows the same data, limited by the admin's scope. Counts are provided for: • online and offline machine agents, both permanent and temporary • KNM assets • total licensed • never checked in
Live Connect	EES-1452	Live Connect now supports navigation of 'symbolic link' folders such as the 'Documents and Settings' folder on Windows 10, 8, 7, and Vista.
Live Connect	AF-2257	Live Connect now supports running on mobile devices such as tablets. Use the following URL format to log into Live Connect: http://www.yourcompany.com/liveconnect
Live Connect	END-2163	You can now run 'non-executable' custom extensions. Examples are MSI installation files and Powershell scripts.
Reports	APPF-2556	Updated the default OS score types and weightings in the Executive Summary report to include new OS types. • Win7, Win 8, Win10, 2008, 2012, 2016 (100%) • Vista, XP, 2003 (75%) • Apple OS, LInux (100%) • Other Windows OSs (25%)
Antivirus	EXT-1976	Added back the 'Show Icon In System Tray' option in Antivirus. When changing this option, a reboot is required to take effect.
Antivirus	EXT-2075	When a machine is out of compliance from the profile in the VSA versus the options on the endpoint in Antivirus, clicking the out of compliance icon displays a pop up grid detailing the reasons the machine is not in compliance.
Antivirus	EXT-2801	Antivirus new installs now use version 10.3.0.6294. Antivirus continues to support version 10.2.5.3201 and version 10.2.4.674 installs.
Antivirus (Classic)	EXT-2622	Antivirus (Classic) new installs now use version 10.3.0.6294. Antivirus continues to support version 10.2.5.3201 and version 10.2.4.674 installs.
Antivirus	EXT-2867	A new System Watcher tab was added to Antivirus profiles.
Antivirus	EXT-1601	A new 'Use LAN Updater' checkbox in the Antivirus module enables peer-to-peer file downloading of Kaspersky definition files using LAN

		Cache. The checkbox is located on the Configuration > Settings > Application Settings tab. Before enabling this feature you must:
		Designate an Antivirus-installed machine as a LAN Cache machine using the Agent > LAN Cache page.
		Assign that LAN Cache to other Antivirus-installed machines on the same network, using the Agent > Assign LAN Cache page.
		An additional 'Refresh Lan Updater' button is provided to enable this same feature immediately on new or reconfigured machines. As a precaution, the 'Refresh Lan Updater' function also runs once a day.
Antivirus	EXT-2755	Added the ability to export data from the Antivirus > Machines page.
Anti-Malware	EXT-2757	Added the ability to export data from the Anti-Malware > Machines page.
Anti_Malware, Antivirus	EXT-2379	Added support for Windows 2016 in Antivirus and Anti-Malware.
AuthAnvil	IAMV-4982	Added support for SHA-256 when using Single Sign-On to log into VSA.
Backup	BACKUP-85	You can no longer disable passwords on the Backup Image page.
Cloud Backup	EXT-2439	Added Cloud Backup support for • SQL Server • Exchange • Active Directory
Cloud Backup	EXT-2652	Added an option to install an Acronis client on a VMware VM machine. The VM acts as a VMware relay to the VMware host, and supports the 'Run as VM' feature on the Acronis Cloud Backup website. The 'Run as VM' feature enables an existing backup to be restored as a new VM on the VMware host machine. • Added an option to install an Acronis client on a Hyper-V host machine, to support the 'Run as VM' feature on the Acronis Cloud Backup website. The 'Run as VM' feature enables an existing backup to be restored as a new VM on the Hyper-V host machine.
Cloud Backup	EXT-2621	You can now filter the 'Last Backup Column' on the Cloud Backup > Machines page using a drop-down list showing the following options: Not Scheduled, Successful, Failed, Delayed, Running,Canceled.
Cloud Backup	EXT-2746	Added an install option to enter administrator-level credentials, if required by the endpoint to install Acronis Cloud Backup client.
Cloud Backup	EXT-2944	Added monthly storage usage by machine and backup group.
Cloud Backup	EXT-2946	Cloud backup report parts now show separate data for cloud storage and gateway storage.
Cloud Backup	KCB-402	A new Acronis Alert History page has been added. The retention period is specified using a new Settings > Global Settings > 'Acronis Alert History Retention Period' option. The default is 120 days.
Cloud Backup	EXT-3110	Added support for scoping and filtering on the Acronis Alert History page.
Cloud Backup	AF-2505	When installing Cloud Backup on multiple servers with the same supported application backup option, a link displays. Clicking the link shows the set of machines that includes this application backup option. This patch hides the link when only one selected machine supports the application backup option.
Cloud Backup	KCB-410	Added an alert to notify administrators that a user has uninstalled the Cloud Backup client from the agent.

Network Monitor	KNM-785	For all Network Monitor performance monitors that have instances, instances are now automatically scanned as soon as you add the monitor.

Service Desk	EXT-2201	Added a new SendPost() command to service desk procedures. The SendPost() creates a POST request and sends it to a specified URL. The request always sends the content you enter in json format.
		
		• If the command specifies a series of fields and values in json format, then running the command sends a POST request formatted as follows:
		`{"PartitionId":"<paritionId>",`
		`"ServerName":"<server`
		`name","ProcedureName":"<procedure name>",`
		`"MyField1":"<myField1>",`
		`"MyField2":"<myField2>",`
		`... }`
		
		• If the command specifies just text, then running the command sends a POST request formatted as follows:
		`{"PartitionId":"<paritionId>",`
		`"ServerName":"<server`
		`name","ProcedureName":"<procedure name>",`
		`"PostData":"<Text to be sent>"}`
		
		The target URL receives this string and processes it.

Software Management	SDP-2916	A new 'Disconnect from Patch Mgmt' button has been added to the Software Management > Machines page. • A newly added 'Attached to Patch Management' column indicates if an agent is currently being managed by Patch Management. • Selecting the 'Disconnect from Patch Mgmt' button disconnects selected agents from being managed by Patch Management. • Selected machines managed by Patch Management because of a Policy Management policy are ignored when using this button.

Bug Fixes

Agents	EES-108	Enabled concurrent scheduling of Lua scripts.
Agents	DISMON-1281	Fixed an issue that prevented custom icons from getting pushed to the correct folder on the agent, unless they were installed using Discovery.
Agents	EES-246	Fixed an issue with KLC, KRC, KAV and KAM not working as expected, if an agent account was deleted without uninstalling the agent and the agent checked back in, creating a new account.
Agents	EES-264	Fixed an issue which could cause the Endpoint to terminate if a task was canceled while the task package was still being downloaded.
Agents	EES-1017	This fix prevents Kaseya Endpoint Services from shutting down if an invalid cron statement is encountered.
Agents	EES-1136	KLC, KAV and KAM did not work if outbound ports 80 and/or 443 were blocked on the agent. This has been fixed.
Agents	EES-1207	In rare circumstances file uploads from an endpoint might cease if one upload completed just as another was requested. This could cause endpoint pending actions not to complete. This has been fixed.
Agents	EES-1212	Fixed an issue that, in rare circumstances, could cause unknown files to be uploaded from the endpoint and be given duplicate names. In some cases, VSA tasks might not complete because of this issue.
Agents	VAKF-1296	The agent version number was updated to 9.4.0.2 for Windows, Linux and Mac machines.
Agents	VAKF-1087	If connection with the KServer is lost during a long-running agent procedure, the agent no longer waits for the procedure to complete before attempting to reconnect.
Agents	VAKF-497	WriteFile (Transfer to file from VSA to agent) could run slowly if many WriteFile operations to different agents were being processed simultaneously.
Agents	SDP-1981	Fixed an issue with auto download failing when the 'Deploy Agent URL' link is accessed.
Agents	SDP-1896	Added named views to include Windows Server 2016.
Agents	SDP-1344	Fixed an 'error loading the dialog' message that could display when selecting the Agent > Manage Agents > Update Agents option.
Agents	END-2187	Curl.exe was updated to fix an issue with agents not checking in when TLS 1.0 was disabled.
Agents	END-2175	Fixed an issue that caused TaskRunner to occasionally terminate during shutdown.
Agents	END-2091	Fixed an issue with continuously-running tasks not being restarted after being updated.
Agents	END-2019	Fixed an occasional KaseyaEndpoint termination caused by an Access Denied error when cleaning up a TaskRunner temporary folder.
Agents	SDP-1441	Fixed an issue with the merging of agent accounts not including custom fields.
Agents	SDP-1443	The Agent > Manage Packages > Create Package wizard no longer displays the Existing Group option, if no machine groups are visible in the current scope.

Agents	SDP-1797	Fixed an issue with missing options on the Agent > Manage Agents > Manage menu.
Agents	SDP-1835	Eliminated the display of multiple entries for 'Package - Create Default Package' in a tenant partition on the Agent > Administration > Application Logging page.
Agents	SDP-1858	Fixed an issue with the Configuration Changes log showing a blank log entry when an agent is moved to new machine group.
Agents	SDP-1864	The Agent > Agent Logs > Diagnostic Logs tab > Endpoints tab > Endpoint log now displays within a classic window polling dialog.
Agents	SDP-1865	Fixed an issue that ensures the agentmon and endpoint logs always display in the new Agent > Agent Logs > Endpoint Logs tab, even if the agent module itself is not activated in a tenant partition.
Agents	SDP-1894	Auto-refresh was removed from the Agent Logs page.
Agents	SDP-1899	Fixed an issue manually updating Linux agents to the latest agent version on the Agent > Manage Agents page.
Agents	SDP-1958	Fixed the total page count on Agent > Agent Log tabs, to accurately show counts greater than 1 when appropriate.
Agents	SDP-1982	Offline agents no longer display the 'Agent Mon' and 'Kaseya Endpoint' logs.
Agents	SDP-2022	Reopening the Agent > Manage Agent > Update Agents dialog no longer shows an agent procedure selected in the 'Agent procedure to run after the update' field, based on the last time you ran agent update.
Agents	SDP-2024	Fixed an issue with returning the correct machine count on the Manage Agents page when filtering the page using the Credentials column filter.
Agents	SDP-2046	Fixed an issue that prevented adding the SQL Server 2005 label to an agent view definition. The selection was not saved.
Agents	SDP-2055	Updated the Agent > Packages > Manage Packages dialog to display the correct switches on the second page, after clicking the Previous button and selecting the 'Specify how the group id is assigned' option on the first page and click Next to show the second page again.
Agents	SDP-2104	Added support for Windows Server 2016 on the Agent > Automatic Agent Update page.
Agents	SDP-2522	Fixed an error that displayed when clicking the set credential key icon to open the set credential dialog on the Agent > Manage Agents page.
Agents	SDP-2532	Fixed an issue with Agent Auto Update not working on Server 2016.
Agents	SDP-2615	Fixed an issue with Automatic Agent Update not skipping offline agents.
Agents	SDP-2636	Fixed the display of the Download Package dialog when trying to display it using https and an IP address.
Agents	SDP-2649	All actions on the Agent > Manage Packages page are now only enabled when a single row is selected.
Agents	SDP-2798	Fixed an issue that prevented resuming suspended agents when the agent list is filtered to only show suspended agents.
Agents	SDP-2812	You can now clear credentials when using a credential grid column filter.
Agents	SDP-2994	Fixed an issue that caused the Agent > Agent Logs > VSA Technician > Live Connect Logs tab to display no data.

Agents	SDP-3050	Fixed the Set Credential dialog to ensure only selected rows are displayed.
Agents	SDP-3192	Added validation to prevent creating agent packages with the same name.
Agents	SDP-2069	Fixed an issue that prevented policies from taking effect after assigning a machine to a different machine group.
Agents	APPF-2234	Fixed an issue deleting screen recording from Agent > Agents > Screen Recordings page.
Agents	AF-2265	Fixed an issue with using a view definition that filters by machine group when the number of machine groups exceeds 100.
Agents	EES-1235	In some cases the endpoint might attempt to download files before it had completed authentication, which would result in the downloads failing. This has been fixed.
Agents	SDP-1683	Added a black list mechanism to prevent unsupported operating systems from being updated to the latest agent using Automatic Agent Update.
Assets	APPF-2547	Machine group changes are now propagated to non-agent assets.
Agent Procedures	EES-1410	Fixed an issue that prevented the writeFile() step in an agent procedure to not use LanCache.
Agent Procedures	EES-999	Fixed an issue that could cause the agent to terminate when running an agent procedure with a getVariable() command that specified a long filename.
Agent Procedures	SDP-1547	On the Agent Procedures > Schedule / Create page, the text displayed when the Shared cabinet is selected was updated.
Agent Procedures	SDP-2506	Fixed an issue that sometimes incorrectly loaded the system scripts and broke the path to curl. This patch prevents the issue from happening to systems that have not already installed 9.4.0.10, but will not fix already broken systems. For already broken systems, running reinstall database schema is the recommended fix.
Agent Procedures	SDP-2541	Fixed an agent procedure folder import issue when the folder already exists.
Agent Procedures	SDP-3101	Fixed an issue that prevented downloading a GetFile document using the Quickview > Get File option, after installing patch 9.4.0.21.
Agent Procedures	AF-2280	The Agent Procedure > Schedule / Create page now refreshes immediately when a machine group or view is selected, instead of requiring the page be refreshed manually.
Agent Procedures	SDP-1325	Manage variables now support values that include single and double quotes.
Audit	EES-65	Fixed an issue with audits not detecting the Office 2013 product key.
Audit	VAKF-919	Fixed an issue auditing a machine with more than 32 logical CPUs.
Audit	DISMON-1672	Fixed an issue with the latest audit not identifying installed applications correctly.
Audit	SDP-1334	A new 'Latest Audit Date' column was added to the Applications report part.
Audit	SDP-1469	Updated the getvariable() step to run on all OSs, not just Windows.
Audit	SDP-1519	Fixed an issue filtering by the agent status icon on the Audit > View Individual Data > Machine Summary page.
Audit	VAKF-605	Some installed programs that do not have an uninstall option were not being displayed in Audit Add/Remove. BackupAssist is one such program.

		This has been fixed.
Classic Monitoring	DISMON-1283	Fixed an issue with classic Monitoring not working when applied to Server 2016 agents.
Kaseya Remote Control	EES-205	Rebooting an agent machine from the desktop within a KRC session now displays a 'Session Ended' message.
Kaseya Remote Control	EES-856	The user is now prompted to enter an admin note, if required by policy, when launching KRC directly by clicking the agent icon in the VSA.
Kaseya Remote Control	APPF-2575	Fixed an issue that caused the Legacy Remote Control Log report part to show Kaseya Remote Control log entries.
Kaseya Remote Control	SDP-2035	Fixed the link to online help when attempting to Kaseya Remote Control to an unsupported OS.
Kaseya Remote Control	EES-260	Fixed an issue that prevented stopping the KRC 'Recording' button after it was started.
Kaseya Remote Control	EES-263	When launching KRC from the VSA and the connection policy requires user approval, the connection window now shows the message "Awaiting User Approval...".
Kaseya Remote Control	EES-1045	Fixed an issue with Kaseya Remote Control sessions not showing the active admin on the Remote Control > Control Machine page.
Kaseya Remote Control	EES-1047	Live Connect sessions and Kaseya Remote Control sessions now always open in the foreground. Previously, sessions could open in the background.
Kaseya Remote Control	EES-1051	Fixed an issue with high latency on relayed remote control sessions.
Kaseya Remote Control	EES-1056	Fixed an issue with stuck mode keys--shift, control, caps lock, for example--during Kaseya Remote Control sessions.
Kaseya Remote Control	AF-2786	Launching Kaseya Remote Control now displays a message if the user does not have access to the Audit module. Previously, the session would hang without telling the user access was required.
Kaseya Remote Control	EES-191	This fix ensures desktop objects within the KRC window respond to click events immediately, without having to click the KRC window once to regain cursor focus.
Kaseya Remote Control	EES-196	Fixed an issue with shared sessions that caused KRC to sometimes show a black screen after CTRL+ALT+DEL was entered on the remote machine. Previously, the user would have to close KRC and reconnect to display the remote desktop correctly.
Kaseya Remote Control	EES-798	The Kaseya Remote Control window no longer flickers as it opens when clicking the agent status icon to launch it.
Kaseya Remote Control	EES-836	Fixed an issue that prevented Kaseya Report Control private sessions to Window 10 machines with certain security settings in place.
Kaseya Remote Control	EES-1001	Launching a KRC session outside of Live Connect now prompts you to download the latest version available.
Kaseya Remote Control	EES-1003	Added back support for Ctrl + Alt + Ins acting as a replacement for Ctrl + Alt + Del in Kaseya Remote Control sessions.
Kaseya Remote Control	EES-1113	Provided an optional configuration for remote control sessions that show a black screen on some administrator machines. When this occurs, configure the following on the affected administrator machine you are running Live

		Connect from.

		Enable SW rendering by adding the following two lines to the `%APPDATA%\Kaseya\KaseyaLiveConnect.ini` file. If the file doesn't already exist, create it using a text editor.
		`[Renderer]`
		`UseSWRenderer=true`

Kaseya Remote Control	EES-1298	Fixed an issue with notifying users when a session terminates using Kaseya Remote Control.
Live Connect	EES-230	Fixed an issue that prevented uploading of files to Live Connect custom extensions.
Live Connect	AF-2138	Fixed an issue with Live Connect becoming unresponsive when transferring large files.
Live Connect	AF-2339	Added Live Connect Mobile support for iOS and Android phone resolutions and other minor enhancements.
Live Connect	AF-2461	Live Connect fatal errors now only terminate the specific tab affected. Other open Live Connect tabs will remain connected.
Live Connect	AF-2491	Fixed an issue that caused the file transfer progress bar window in Live Connect > File Manager to be incorrectly positioned after minimizing and restoring the progress bar window.
Live Connect	AF-2494	When setting the filtered view in the Live Connect asset browser, then logging off then back on again, the filtered view now resumes immediately.
Live Connect	AF-2536	Fixed an issue with scrolling multiple pages using the Live Connect > Events page.
Live Connect	AF-2579	Fixed an issue with unscrollable drop-down menus in Live Connect Mobile.
Live Connect	AF-2608	Fixed an issue with the Live Connect > Events page showing a blank page when scrolling to the end of the list.
Live Connect	AF-2637	Fixed an issue that caused multiple Live Connect sessions to max out the number of concurrent user sessions allowed for a VSA user role.
Live Connect	AF-2765	Fixed an issue with typing text into the search box of a new tab in the Live Connect window, after launching a remote session.
Live Connect	AF-2782	Fixed an issue causing crashes on Mac machines when trying to use Live Connect.
Live Connect	AF-2892	All event fields have been added to the Live Connect > Events grid, so the user is not forced to display the popup dialog for a single row to view event details.
Live Connect	AF-2894	Live Connect now displays the full path name of a process in the Processes detail dialog.
Live Connect	AF-2895	Added the ability to multi-select files and folders.
Live Connect	EES-730	Updated the title bar of Live Connect to display the VSA server name/IP address.
Live Connect	EES-1060	Optimized the downloading of large files from Live Connect to prevent locking up the app.
Live Connect	EES-1548	Fixed a looping 'permission denied' message that could display opening LIve Connect.
Live Connect	EES-175	Fixed the display of an application error when clicking the Events tab of Live Connect.

Live Connect	EES-189	Fixed a 'Permission Denied' error when trying to access the Microsoft branch using the Registry page in Live Connect.
Live Connect	EXT-1806	Live Connect no longer deletes the submitter information you just entered in a new Ticketing ticket when you change categories.
Live Connect	END-2141	Fixed an issue that prevented uploading of files to Live Connect custom extensions.
Live Connect	AF-2283	Fixed an error in Live Connect when downloading files with special characters in the filenames.
Live Connect	EES-218	Fixed an issue that prevented a custom extension from executing if, when downloaded and run, there happened to be another file in use with the same name in the same directory.
Live Connect	EES-271	Rebooting an agent machine from the desktop within a KRC session now displays a 'Session Ended' message.
Live Connect	EES-217	Fixed an Application Error in Live Connect related to an invalid date time format, associated with installing the Kserver on an Italian Windows Server.
Live Connect	EES-182	This fix ensures the 9.4 Live Connect > Command Prompt shell will work with a 9.3 agent that hasn't been upgraded yet. Requires upgrading the agent.
Live Connect	ESR-514	It is now possible to terminate processes running under LocalSystem on Windows hosts in the LiveConnect UI.
Live Connect	EES-259	Fixed a rare issue which could cause the endpoint to terminate during a live connect session
Live Connect	AF-2768	Fixed an issue with Live Connect running after the first attempt on non-English servers. The following message displayed: "Unable to locate an I18n file for culture code..."
Live Connect on Demand	SDP-1619	For SaaS users only, the URL used by machine users to download a temporary agent install package has been changed to 'https://liveconnect.me'. This setting displays on the Agent > Live Connect on Demand > Configuration page. On premise systems will continue to use a link to the local version of ARS.
Live Connect on Demand	SDP-1787	The email invitation to machine users to install a temporary agent now includes a reminder that the install link will expire in specified time period.
Live Connect on Demand	SDP-1933	The field name 'ARS URL' was changed to 'URL' on the Agent > Configuration > Live Connect on Demand page. It also now displays consistently.
Live Connect on Demand	SDP-2021	Fixed an issue that prevented enabling Live Connect on Demand on a SaaS trial server.
Live Connect on Demand	SDP-3043	Fixed an issue with 'Live Connect on the Demand' agents not displaying their badge on the Audit > Asset > Manage Credentials page.
Live Connect on Demand	SDP-1630	Installing an IIS WebDAV module, no longer interferes with PUT and DELETE methods in an on premises ARS.
Live Connect on Demand	SDP-2064	Added support for either HTTP or HTTPS being required or optional when running Live Connect on Demand, based on how the web server is configured.
Live Connect on	SDP-1649	Added a 'Live Connect on Demand' sample icon to the legend on the

Demand		Remote Control > Control Machine page.
Quickview	SDP-3154	Fixed an issue that prevented downloading a file from Quickview that contains a % in the filename.
Quickview	APPF-2370	Fixed the calculation of the 'user inactive since' time displayed in the titlebar of the Quickview window.
Quickview	APPF-2474	Fixed an issue with the Quickview > Procedure History list showing events in Kserver time instead of the preferred time set on the System > Preferences page.
User Portal	ATTHREE-491	Fixed an issue with User Portal not honoring custom web server ports.
User Portal	AF-2347	Fixed an issue with the Agent Procedures page in User Portal not loading in Firefox.
User Portal	AF-2403	Fixed an issue that prevented Live Connect > Chat from working if a custom 'Contact Administrator' URL was specified using the Agent > Configure Agents > Agent Menu page.
User Portal	AF-2407	User Portal now displays the name of the agent in the title bar.
User Portal	AF-2411	When starting a Live Connect > Chat session from a VSA using https, the User Portal session that opens on the endpoint machine now also launches using https. Previously it launched using http.
User Portal	ATTHREE-496	User Portal menu items will now reflect all machine role settings.
Reports	APPF-2304	Fixed a timeout issue generating the executive summary report when the uptime log contained a large volume of agent data.
Reports	APPF-2663	Fixed a problem with dynamic views causing reports to fail.
Reports	APPF-2230	Fixed an issue with header logos being cropped in published reports.
Reports	APPF-2390	In report schedule/run now dialogs, the 'no view selected' option is now at the top of the list of the view combo box.
Reports	APPF-2414	The timestamp shown when a report is published now reflects the preferred time set on the System > Preferences page.
Reports	APPF-2504	SSRS 2012+ now renders Excel as .xlsx instead of .xls
Reports	EXT-1541	Fixed an issue with using three name value parts in reports: • AM Installation Count • AM Installation Count (Servers) • AM Installation Count (Workstations)
Reports	SDP-2039	Added a missing machine group and organization filter dialog for previewing a configured Agent > Machine Group Deploy URL report part.
Reports	SDP-2714	Added a fix that ensures the Executive Summary report can be run whether the Software Management module is installed or not.
System	APPF-1551	Fixed an issue that prevented non-master admins from renaming machine groups.
System	APPF-2543	Fixed an issue with graphs on the System > Statistics page not showing data when using SQL Server 2016.
System	APPF-2487	Fixed an issue with context errors displaying when trying to access the System > License Manager page in a tenant.
System	APPF-2192	Added a fix to prevent the propagation of duplicate entries when copying permissions between machine roles.

System	APPF-619	The Kserver is no longer restarted after applying a new license, when the only change is to add additional agents. This was causing the Kserver to be offline unnecessarily.
System	APPF-2056	In tenant partitions, the System > User History page now shows the user history for all users, not just System users.
System	APPF-2114	Fixed an issue with log archiving that was causing the archive process to not have the proper permissions to complete the operation.
System	APPF-2151	Fixed a half-hidden bottom scroll bar on the System > System Log page.
System	APPF-2165	Updated the System > Logon Policy page to accept decimal input for number of hours to disable the account after max logon failures exceeded. Example: 0.5.
System	APPF-2166	Fixed an issue with the VSA SQL backup retention policy not being honored causing servers to run out of storage.
System	APPF-2203	Fixed an issue with the System > License Manager > Role Types tab not loading when Max Concurrent Licenses is set to NULL
System	APPF-2350	When a tenant updates the Logon Policy page to require a password change every X days, new users created after the Logon Policy change are set to start counting their days from the date they first logon, and not forced to change their password the first time they logon.
System	APPF-2378	The drop-down lists for Country and US State in the System > Orgs/Groups/Depts/Staff > Manage page now display in alphabetical order.
System	APPF-2381	Fixed the display of the addon version number for System Backup and Recovery and Cloud Backup. on the System -> License Manager page.
System	APPF-2386	Added a system log entry to document when the 'Automatically redirect to https at logon page (except when accessing via localhost)' checkbox is checked or unchecked on the System > Server Management > Configure page.
System	APPF-2075	Fixed an issue with server notification messages not honoring the time zone offset on the System > Preferences page.
Ticketing	EES-164	Fixed an issue that caused the file attachments of inbound Ticketing emails to be empty if the file name contained an empty space.
Ticketing	EXT-1803	Deleting tickets using the Ticketing > Delete/Archive page now removes corresponding records from the `ticrequest` and `ticRequestTicket` database tables.
Ticketing	EXT-1810	Fixed a scope issue when multiple instances of a customized ticket report for different organizations were executed at the same time.
Ticketing	EXT-1933	Fixed an issue that prevented opening a ticket using the Ticket link embedded in a notification email.
Ticketing	EXT-2797	Fixed an issue with Ticketing tickets created from inbound email with attachments showing HTML tags in the ticket.
Notification Bar	APPF-2444	Fixed an issue with admin notifications not displaying on the notification bar when a new VSA patch release is available.
VSAPres	AF-2281	The following user interface improvements were made: • When selecting multiple rows in a selector grid, the selection panel--which typically shows details when a single row is selected--now says 'n rows selected'.

		• The new Agent > Screen Recordings page no longer displays a slightly cropped 'Total File Size' row when there are no items in the grid. • Clicking the X buttons for the Machine Group and View combo boxes in the machine group / view filter now redisplays the default watermarks <All Machine Groups> and <No View> values as expected.
VSAPres	AF-2249	A new option has been added to the System > Default Settings page" 'Replace KRC with RC in KLC to allow you to enforce all screen sessions getting recorded' - Yes by default. If Yes, clicking an agent status icon runs Kaseya Remote Control 9.4, which includes the option of recording a session. If No, clicking runs legacy Kaseya Remote Control, which does not include the option of recording a session.
VSAPres	AF-2244	Fixed an issue establishing a connection when launching Kaseya Remote Control from Portal Access.
VSAPres	AF-2210	Set an 500ms interval on the navigation tree to prevent mouseOut events from collapsing the tree.
VSAPres	AF-2496	Fixed an issue dragging & dropping tree pane items into an empty folder.
VSAPres	AF-2515	Fixed a loading error that could occur on any page that contained a pie chart.
BMS Integration	VAKF-1320	Fixed an issue creating tickets using BMSi/VSA integration in a tenant partition.
Kinstall	APPF-2396	KInstall > System Check now ignores the `KLCAuditReporting` database when checking for the presence of multiple databases.
KServer	APPF-2305	Fixed a rare condition where a Kserver outage could cause scripts being scheduled far into the future.
KServer	VAKF-1227	Fixed a log buffer issue that caused KServer to terminate.
KServer	VAKF-1363	Fixed an invalid parameter on a C Runtime function that could cause the KServer to terminate.
Kserver	END-1948	Fixed an issue that could sometimes cause the Kaseya Edge service to terminate unexpectedly on SaaS servers.
Kserver	APPF-2138	Fixed an issue that could prevent the plugin host from fully initializing, causing message queues to stack up.
REST API	APPF-2264	Added a `DELETE /assetmgmt/assets/{assetId}` REST API.
REST API	API-535	The following deprecated REST API resource routes have been added to 9.4. When a valid authenticated request is made to these routes, the response contains a Location header with the updated location for the resource. Most user agents will automatically reissue a request to the new URL in the Location header, returning a response from the new route without interruption to the client. • `GET /automation/servicedesk` - redirects in 9.4 to `GET /automation/servicedesks` • `GET /automation/servicedesk{serviceDeskId}/tickets` - redirects in 9.4 to `GET /automation/servicedesks/{serviceDeskId}/tickets` • `GET /automation/servicedesk/{serviceDeskId}/ticketstatus` - redirects in 9.4 to `GET /automation/servicedesks/{serviceDeskId}/status`

		These deprecated resources are not visible in Swagger in 9.4 but can continue to be used.
REST API	API-538	Fixed filtering of categories and priorities by service desk using, for example, the following REST APIs: • `GET /automation/servicedesks/{serviceDeskId}/categories` • `GET /automation/servicedesks/{serviceDeskId}/priorities`
REST API	APPF-2268	Added a `DELETE /assetmgmt/agents/{agentId}/{uninstallfirst:bool?}` REST API.
REST API	APPF-2412	Updated the documentation for the REST API `PUT /automation/agentprocs/{agentId}/{agentProcId}/schedule` to describe the parameter values to enter for recurring schedules.
REST API	APPF-2445	Fixed an issue with updating a VSA user record using the `PUT /system/users/{userId}` REST API.
REST API	API-382	Fixed an error that could display when selecting the Live Connect > Log Viewer > Agent Logs page.
REST API	EXT-2794	Added a filterable Archived property to the `GET /automation/servicedesks/{serviceDeskId}/tickets` REST API.
Database	APPF-2302	Optimized SQL views to prevent views timing out on high volume systems.
Database	APPF-2392	Improved the performance of returning data using the `vPatchStatusByAgent` view.
Database	APPF-2480	Created clustered primary keys on dated log files for performance and to help prevent locking.
Database	APPF-2541	Fixed an issue that prevented the creation of the appropriate database views when importing customer content packs using the Import Center.
Database	APPF-2318	Fixed an issue with agent signing failing when a large number of rows exist in the scriptlog for a specific agentguid.
Security Vulnerability	SDP-2841	A security vulnerability was removed.
Security Vulnerability	SDP-1686	A security vulnerability was removed.
Security Vulnerability	APPF-2466	A security vulnerability was removed.
Security Vulnerability	EXT-2733	A security vulnerability was removed.
Security Vulnerability	APPF-2576	A security vulnerability was removed.
Security Vulnerability	API-474	A security vulnerability was removed.
Security Vulnerability	AF-2568	A security vulnerability was removed.

Security Vulnerability	AF-2569	A security vulnerability was removed.
Security Vulnerability	AF-2571	A security vulnerability was removed.
Security Vulnerability	APPF-2428	A security vulnerability was removed.
Security Vulnerability	APPF-2429	A security vulnerability was removed.
Security Vulnerability	APPF-2430	A security vulnerability was removed.
Security Vulnerability	APPF-2431	A security vulnerability was removed.
Security Vulnerability	APPF-2432	A security vulnerability was removed.
Security Vulnerability	APPF-2433	A security vulnerability was removed.
Security Vulnerability	APPF-2435	A security vulnerability was removed.
Security Vulnerability	APPF-2436	A security vulnerability was removed.
Security Vulnerability	APPF-2437	A security vulnerability was removed.
Security Vulnerability	APPF-2438	A security vulnerability was removed.
Security Vulnerability	APPF-2439	A security vulnerability was removed.
Security Vulnerability	APPF-2440	A security vulnerability was removed.
Security Vulnerability	APPF-2441	A security vulnerability was removed.
Security Vulnerability	APPF-2484	A security vulnerability was removed.
Security Vulnerability	DISMON-1502	A security vulnerability was removed.
Security Vulnerability	EES-1311	A security vulnerability was removed.
Security Vulnerability	EXT-2730	A security vulnerability was removed
Security Vulnerability	EXT-2735	A security vulnerability was removed.
Security Vulnerability	EXT-2738	A security vulnerability was removed
Security Vulnerability	EXT-2739	A security vulnerability was removed
Security	EXT-2741	A security vulnerability was removed.

Vulnerability		
Security Vulnerability	EXT-2782	A security vulnerability was removed.
Security Vulnerability	SDP-2640	A security vulnerability was removed.
Security Vulnerability	SDP-2641	A security vulnerability was removed.
Security Vulnerability	SDP-2642	A security vulnerability was removed.
Security Vulnerability	SDP-2643	A security vulnerability was removed.
Security Vulnerability	SDP-2724	A security vulnerability was removed.
Security Vulnerability	AF-2048	A security vulnerability was removed.
Security Vulnerability	SDP-2047	A security vulnerability was removed.
Anti-Malware	EXT-2113	Fixed an issue that caused Anti-Malware manual scans to not remove found threats.
Anti-Malware	EXT-2180	Fixed a Pending Actions error that prevented an Anti-Malware profile from being applied to a machine. The error states "Could not convert string to DateTime: NaN-NaN-NaNTNaN:NaN:NaNZ. Path 'LastFlashScan', line 20, position 48"
Anti-Malware	EXT-2367	Fixed an issue with Anti-Malware detections not being deleted in the database.
Anti-Malware	EXT-2373	Fixed an issue with the 'reboot needed' flag continuing to display after multiple reboots.
Anti-Malware (Classic)	PROTECT-955	Fixed an issue with the Anti-Malware (Classic) log files not showing entries for manual scans.
Antivirus	EXT-2758	Fixed an issue with the Antivirus 'License Expired' popup message to be displayed inaccurately on Windows 10 machines just after they bootup.
Antivirus	EXT-2882	Fixed an issue which caused Antivirus (Classic) to misidentify Windows Server 2016 as a workstation.
Antivirus	EXT-2164	Fixed an issue with non-ASCII characters in the profile exclusion list corrupting the Antivirus client database.
Antivirus	EXT-2172	Fixed an issue that caused profiles to show out of compliance after running Get Status.
Antivirus	EXT-2177	Fixed an issue that could cause Antivirus to show 'Update Profile' and 'Get Status' as stuck pending actions.
Antivirus	EXT-2378	Fixed an issue with inaccurate database definition dates displaying on the Antivirus > Dashboard page.
Antivirus	EXT-2676	Fixed an issue with machines not installed with Antivirus attempting to configure themselves as Antivirus > LAN Updater clients.
Antivirus	EXT-2787	Fixed an issue that prevented Antivirus alerts for 'Definition not updated in X days' from being generated.

Antivirus	AF-2323	Selected records in a grid will now correctly update the counts when a refresh occurs and there is a filter applied.
Antivirus	PROTECT-967	Fixed the sorting of install status columns in Antivirus (Classic) and Anti-Malware (Classic).
Antivirus	EXT-2122	Fixed an issue with Antivirus scheduling not honoring the timezone offset set on the System > Preferences page.
Antivirus (Classic)	EXT-2225	Fixed an issue returning correct results using the Info Center > Report Part > Anti-Virus > AV Installation Statistics > 'In Installed' column.
Antivirus (Classic)	EXT-2231	Fixed an error that displayed when generating a report that included the 'Active threats Count' column of the 'AV Monthly Count' report part.
Antivirus (Classic)	EXT-2247	Fixed the name value part for the AV Install Ratio used in reports.
AuthAnvil	IAMV-5085	Applies to SaaS only. Fixed an issue with the postback event failing when logging on with 2FA enabled and providing a passcode.
Backup	BACKUP-390	Fixed a timeout error displaying log files on the Backup Logs page, when a large number of backups are schedules to run.
Backup	BACKUP-380	The VSA > Backup client installer was upgraded to Acronis version 11.7-50214.
Backup	BACKUP-375	Fixed an issue that prevented Acronis from skipping or scheduling a backup If one was already running. This caused alert notifications to not be generated.
Backup	EXT-2285	Fixed a schema error that occurred if 'Backup Disaster Recovery' was not selected during Kinstall.
Backup	EXT-2776	Fixed an issue that caused synthetic full backups to fail on Acronis 11.7 clients.
Cloud Backup	KCB-413	Added support for using Acronis Cloud Backup credentials that connect with the Acronis data center in Switzerland.
Cloud Backup	KCB-411	Fixed the method used to update Last Backup Time.
Cloud Backup	EXT-2912	Added extra validation to prevent machines from disappearing from the Acronis website when the same Acronis account is used in multiple VSAs.
Cloud Backup	EXT-2935	Fixed a timeout issue with installing the Cloud Backup client in some environments.
Cloud Backup	EXT-2430	Fixed an issue that limited the number of times the Cloud Backup client could be installed on a machine.
Cloud Backup	EXT-2440	The Install button for Cloud Backup was renamed 'Install/Upgrade Acronis Agent' to indicate both tasks can be performed by the same dialog.
Cloud Backup	EXT-2707	Fixed a license count issue for VMs in Cloud Backup.
Cloud Backup	EXT-2728	Fixed an issue syncing the "Last Backup Status" and "Last Backup Date" columns on the Cloud Backup > Show > Machines page with data shown in the Acronis console.
Cloud Backup	EXT-2881	Fixed an issue displaying data using the Cloud Backup > Monthly Storage Usage report part.
Cloud Backup	EXT-2942	Fixed an issue with the Backup Groups page not honoring the scope of the user and showing all machine groups when Backup Group Mapping is set to organizations.
Cloud Backup	EXT-2965	Fixed some issues with the collection of backup data caused by old

		activities hat don't exist anymore.
Cloud Backup	EXT-2968	Fixed the line wrap of advanced install options in the KCB install dialog.
Cloud Backup	EXT-3055	Fixed an issue displaying the correct last harvest time on the dashboard.
Data Backup	BACKUP-247	Fixed an error message that displayed in Data Backup when scheduling backups to run on 100+ machines - "There was a problem : transaction aborted".
Desktop Management	SDP-2478	Applying a printer policy to a machine no longer hangs if the machine does not have the driver for a specified printer installed.
Desktop Management	NSM-1746	Fixed an issue with periodic Desktop Management audits failing.
Desktop Management	NSM-1751	Outdated links on the Desktop Management > Overview page were removed.
Discovery - Domain	DISMON-1224	Fixed a timeout issue scanning Discovery domains when processing a large dataset.
Discovery - Domain	DISMON-1475	Fixed an issue auto-deploying a large number of agents concurrently from the Discovery module.
Discovery - Network	DISMON-1274	Fixed the display of the 'Power-Other' type icon on the Discovery > Discovered Devices page.
Discovery - Network	DISMON-1512	Fixed an issue that prevented a subsequent Discovery Network scan from being run after the initial scan was interrupted and the probe agent swapped with another agent.
Discovery - Network	DISMON-1269	Added a fix to ensure upgrading from earlier versions of Discovery does not prevent the deletion of discovered devices.
Discovery - Network	AF-2551	Fixed a page layout issue. The machine filter options were cropped on the following pages: • Discovery > Networks > By Network • Discovery > Networks > Discovered Devices • Discovery > Networks > Discovered Devices - Tile View
Endpoint Security	EXT-493	The Endpoint Security password is now required to access the 'Temporarily disable AVG protection' option on AVG 2016 clients.
Endpoint Security	EXT-1845	Fixed a mapping issue between profile settings and AVG client settings, for Email and Link Scanner components.
Endpoint Security	EXT-1872	Fixed an issue that caused Endpoint Security profiles to fail to be applied if the profile's Resident Shield tab specified file extensions that were longer than 4 characters or had an asterisk (*) prefix.
Endpoint Security	EXT-2106	Resized agents Icon on the Security > Configure > Installations page.
Endpoint Security	EXT-2136	This fix ensures Endpoint Security does not re-download the client install package when it is already available in the correct download directory on the agent machine.
Endpoint Security	EXT-2143	Fixed a .NET version mismatch error that could cause Endpoint Security pages to fail to load.
Endpoint Security	EXT-2183	Fixed two issues: • The AVG 2016 Firewall component is now disabled on all new installs. • Disabling the Email Scanner component no longer causes an install to show as 'not fully protected'.

Endpoint Security	EXT-2398	Improved the filtering of AVG installed security products, to prevent baseline audits from showing AVG installed multiple times.
Endpoint Security	EXT-2437	Disabled the display of unnecessary AVG 2016 system tray notifications and advertising to the machine user.
Endpoint Security	EXT-2671	Endpoint Security no longer shows a 'Failed to Apply' profile message after the first reboot following a new installation.
Endpoint Security	APPF-1705	Fixed an issue with Endpoint Security inaccurate license count usage on the System > License Manager > License by Group tab.
Endpoint Security	EXT-2159	Applies to SaaS only. Fixed an issue displaying the Endpoint Security > View Threats page and View Logs page correctly.
Multi-Tenant	APPF-2149	Multiple concurrent master sessions are now supported for the same master user in Tenant Management.
Multi-Tenant	APPF-2218	The Agent module is now automatically activated when a new tenant is created using Tenant Management.
Multi-Tenant	APPF-2111	Added a new REST API to 'deactivate tenant' rather than remove it: DELETE /tenantmanagement/tenant/deactivate.
Multi-Tenant	APPF-2110	The GET /tenantmanagement/tenant/{tenantId} REST API was updated to return data for the complete set of zzVal attributes.
Multi-Tenant	APPF-2052	Fixed an issue that caused Linux install packages to download an exe file instead of an sh file in tenant partitions.
Network Monitor	DISMON-1452	Fixed an issue with Mail Server QOS monitor reporting round trip time incorrectly if time zone was not UTC.
Network Monitor	DISMON-1474	Fixed Network Monitor license usage counts in tenants.
Network Monitor	EES-1572	Fixed a data issue with KNM system logs in SaaS tenants.
Network Monitor	KNM-548	The MIB Browser now displays the OID number in parentheses next to each OID name in the tree.
Network Monitor	DISMON-1320	Turned off unnecessary informational event log messages sent to the Event Viewer by Network Monitor.
Network Monitor	RELEASE-222	Fixed an issue with the VSA installer including the 32-bit KNM executable instead of the 64-bit KNM executable.
Network Monitor	EXT-2678	Fixed an issue that caused Ticketing tickets created by a KNM action getting assigned to the organization associated with the Discovery network, instead of the organization associated with the asset.
Patch Management	SDP-1240	Fixed an issue that prevented creating a patch policy when the VSA used the Japanese language pack.
Patch Management	SDP-1900	Added support for Windows 2016 to the 'Patch Scan' agent procedure.
Patch Management	SDP-1995	Fixed an issue that prevented patches from installing if Patch Management used LAN Cache as the file source.
Patch Management	SDP-2645	Fixed an issue with Offline Patch Scan not finding installed updates on Windows 10 PCs.
Patch Management	SDP-2966	Fixed a performance and concurrency issue related to the processing of Patch Management approval policies in high volume, multi-tenant environments.
Patch	SDP-427	Windows 10 machines now show correct counts for installed patches in

Management		Patch Management.
Policy Management	APPF-2391	Eliminated the processing of redundant events during policy deployment.
Policy Management	APPF-2314	The performance of the Settings > Compliance Check process across all tenants has been improved.
Policy Management	AF-1432	Fixed an issue with the scheduler for the agent procedure policy setting in Policy Management not honoring the time preference set in System> Preferences.
Policy Management	SDP-2066	Fixed a contention issue that could unnecessarily delay agent policy deployments or compliance checks.
Policy Management	SDP-2070	The Patch Reboot Action schedule in Policy Management now respects the time zone offset.
Policy Management	SDP-2074	Fixed an issue that caused the "Patch Reboot Action > Run procedure after machine is rebooted" field to clear after changing the scheduling of the policy as you save it or copy it.
Policy Management	SDP-2495	Fixed an issue with policy schedules being lost after updating a policy.
Policy Management	SDP-2749	Fixed an issue with saving the patch reboot action in Policy Management.
Policy Management	SDP-3091	Fixed an issue that caused the 'Compliance Check Schedule' and other schedules to be lost after changing the 'Automatic Policy Deployment Interval' option on the Settings page.
Policy Management	SDP-3164	Fixed an issue that prevented the 'Automatic Policy Deployment Interval' option from being saved.
Service Billing	APPF-2219	Fixed an issue that prevented exporting grid data from the Service Billing > Operations > Recurring Services page.
Service Billing	APPF-2379	Fixed an issue that caused a customer record created in Service Billing only displaying as a machine group in Policy Management.
Service Desk	SDP-1855	Fixed an issue that caused the Agent > Agent Logs > Alarm Log tab to be blank when Service Desk was activated to create tickets associated with alarms.
Service Desk	AF-2082	Fixed an issue with scrolling to, and viewing, a large image added to the note of a Service Desk ticket.
Service Desk	EXT-1709	Copying a ticket in Service Desk now includes the submitter's email address.
Service Desk	EXT-1721	Fixed an issue that caused Service Desk mail template variables to not be populated if the access role was set to View Only.
Service Desk	EXT-2101	Fixed an issue with auto-closing of alert-generated Service Desk tickets not working on some systems.
Service Desk	EXT-2140	Fixed an issue that could cause Service Desk tables to lock for several minutes when clicking the Print Ticket option in Service Desk.
Service Desk	EXT-2422	Fixed an issue which caused a TicRequest error when assigning staff to an alert Service Desk ticket.
Service Desk	EXT-2725	Tickets with file attachments created using the Service Desk API now show links to download the file attachments using the Service Desk ticket editor.

Service Desk	EXT-2173	Fixed an issue which could cause Service Desk ticket exports via the System > Import Center page to fail.
Software Deployment	EES-75	Fixed an issue downloading Ninite installers when using the 'Agents Download Installer From: VSA URL' option in the Software Deployment > Application Settings > General Settings > Edit dialog.
Software Deployment	SDP-2574	Updated the text on the Configuration Changes log to correctly report set credential was applied from Software Deployment.
Software Deployment	AF-1467	Fixed an issue that prevent a user from editing the Profile Status list, once the Status column filter was set. This list displays when you click the Status Profile pie chart on the Software Deployment > Dashboard page.
Software Deployment	SDP-1708	Fixed an issue with the Software Deployment > Catalog > Edit Installer: Settings not saving consistently when edited.
Software Deployment	SDP-1709	Fixed an issue installing Opera Chromium in Software Deployment.
Software Deployment	SDP-1862	Changes were made to prevent Software Deployment deadlocks when running baseline audits and applying profiles via policy management.
Software Deployment	SDP-2032	Fixed an issue that prevented running the run latest scan in Software Deployment when the credential filter was set.
Software Deployment	SDP-2756	Fixed a query to return the proper Software Deployment application versions for approval.
Software Deployment	SDP-2896	Fixed an issue that caused Acrobat (Update only) 17.9.20044 to revert back to 11.0.20 when added to a profile that has Auto Approve checked.
Software Deployment	SDP-3195	.NET framework 4.7 is now available in the Software Deployment catalog.
Software Deployment	SDP-2713	Fixed an issue with 'Schedule Deployment Profile Assignment' not applying recurring deployment schedule patterns reliably.
Software Deployment	APPF-2238	Fixed a validation error that could occur when trying to set the Disable Ninite license limit for a tenant in Tenant Management. This license limit is available for customers who wish to use Software Deployment without Ninite Catalogs.
Software Deployment	SDP-1757	Fixed an issue adding the latest version of Adobe Reader DC to the local catalog.
Software Management	SDP-3053	Software Management now requires agent version 9.4.0.12 or later.
System Backup and Recovery	EXT-2651	The following missing options were added to the System > User Roles > Access Rights tab for the System Backup and Recovery module: • Summary • Summary > Overview • Summary > Dashboard • Summary > Dashboard > Go To Profile • Summary > Status

Deprecated or Obsolete Features

Live Connect	AF-2589	The HTTP Tunneling option was removed from the Live Connect > SSH page.
Backup	EXT-2446	The 'Enable Password' checkbox on the Backup > Image Password page was removed, since disabling the password is no longer allowed.
Software Management	SDP-3115	Removed support for Windows XP and Windows Server 2003 machines in Software Management.